**U. S. Secret Service**

# Electronic Crimes Task Force Bulletin

June 2018

*Sharing News among Law Enforcement*


## CURRENT TRENDS

### Business Email Compromise "BEC"

The Financial Crimes Enforcement Network (FinCEN) assesses that money stolen in business email compromise (BEC) schemes was directed to money mule accounts within the United States in nearly 70 percent of 11,404 BEC attempts reported from January 2016 through September 2017. According to FinCEN analysis, fraudsters are likely to use United States accounts to avoid detection by financial institutions and victims. Most of the stolen funds almost certainly leave the United States after one or more electronic transfers or "hops" through domestic mule accounts.

The Business Email Compromise (BEC) is an emerging financial cyber threat in which organized groups have targeted various institutions in the form of companies, non-profits and government organizations. The scheme relies on deceiving the victims through a multifaceted,

sophisticated fraud using hackers, social engineers, pre-established bank accounts and employees that have access to an institution's finances. The suspect(s) are then able to deceive the victim through fake invoices, supervisor impersonation, altered email accounts and other means to convince the victim to wire money to another subject controlled bank account or, in some cases, remove those funds at a domestic bank in the form of a cashier's check. That cashier's check can then be deposited elsewhere, preventing a victim from reversing the wire. **Note that the bank account owner receiving the deposit may or may not be knowingly involved in the scheme.**

A common type of BEC fraud involves Real Estate transactions. The suspects, sometimes through malware or social engineering, are able to determine that a real estate closing attorney is about to close on a home and send the closing funds to their client's bank account. The suspects, using an altered email account made to look similar to the original sender (examples below), then send an email explaining that the bank account number and routing number have changed just days before the transaction. The suspects then provide their bank information, which is then wired by the victim, to the new account. In some cases, funds are wired first to a "middle-man" which can often be an "unwitting" accomplice who thinks that they are working from home or involved in a romantic relationship with one of the suspects and allowing their bank account to be used. Funds are then wired overseas and then a percentage is usually returned to the U.S. suspects.

## WHAT TO DO FIRST:

Law enforcement receives a call from a realtor, closing attorney, home buyer, Chief Financial Officer (CFO) of a business, divorce attorney, settlement and injury attorney, or financial institution, reporting that a victim sent money to an account based on a fraudulent email containing wire instructions. After taking the information, the victim or caller, should be asked to send everything by email to the agent or detective as quickly as possible. Time is of the essence if you hope to recover any funds. Within 72 hours, if the wire hasn't been recalled, you have less than a 9% chance of recovering funds. The following facts should be considered:

1. Gather all wiring instructions sent by the suspects.

2. Determine if the below 3 criteria need to be met for FinCEN to request a financial fraud kill chain (FFKC):

- Wire must go overseas
- Wire must be $50k or more
- Wire must have been sent less than 72 hours ago

If the scenario meets the required criteria listed above, the victim must also acquire the following wire information listed below:

Date of Wire:
Amount of Wire:
Victim Name / Originator:
Victim Bank:
Victim Account #:
SWIFT / IBAN Code:
Beneficiary Account:
Beneficiary Bank:
Beneficiary Name:
Country:

**A summary of the incident and any supporting documentation

When all the data is collected it should be immediately forwarded to the local USSS ECTF office for additional action.

If the matter does not meet the 3 criteria for the FFKC, there are additional steps that can be taken. Please contact the local ECTF for guidance.

## European Union General Data Protection Regulation (GDPR)

On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) became law in all EU member states. The GDPR aims to harmonize digital privacy rules across Europe, which for years had been a piecemeal arrangement of varying national data protection regimes. The GDPR is sweeping and imposes stringent obligations on all companies that gather, process, or hold the personal data of European residents. Failure to comply with the GDPR can lead to multimillion dollar penalties - up to four percent of revenue - for those firms found in violation of the rules.

The GDPR may have an indirect impact on law enforcement investigations due to its limits on commercial collection, processing, storage, and transfers of personal data, despite its derogation for public interests. One area this is being seen is in access to personal data contained in the WHOIS system, the decades' old mechanism for keeping public records of who owns and operates the millions of Internet domain names and a key source of investigative information to identify who owns and operates a website. The European Union's association of data protection authorities - known as the Article 29 Working Party - indicated in April 2018 that the collection and publication of WHOIS information pertaining to EU residents is in conflict with the GDPR and that firms that continue to provide that information to the public could be subject to severe penalties. In response, many domain name owners and operators have begun to withhold WHOIS information from public access, thus threatening the ability of law enforcement officials to conduct early stage research without the use of a subpoena, as was the prior practice.

The U.S. Departments of Commerce, State, and Justice have been working with the European Commission and the Internet Corporation for Assigned Names and Numbers (the California non-profit that coordinates the WHOIS system) towards a solution. However, no agreement has yet been reached. U.S. Secret Service's Office of Investigations is working with DOJ to ensure we maintain timely access to full WHOIS data. Negotiations are ongoing, both domestically and in Europe.

If you have any questions related to general data protection regulation (GDPR) please contact your local USSS ECTF who can provide additional information from our Global Investigative Operations Center (GIOC).

## Malware Vectors

The Verizon Data Breach Investigations Report (DBIR) annually reports on the most common functionalities of malicious code in real-world security incidents and data breaches. Not only is it important to have awareness about what malicious code is trying to accomplish but also to know how the malware is installed in the first place. We track this by the VERIS enumeration malware vector. The top three vectors over the last three years are as follows:

1. Email (64%)
2. Direct install - installed after device compromise (28%)
3. Web drive-by (5%)

Malware via email is the top vector for malware installation according to our data. Moreover, we are able to validate our findings by tapping into another data set completely independent of our corpus. We received millions of instances of malware attacks and over 90 percent were email-based, (with about 6 percent being web-based and 1% other). It is imperative that a high level of scrutiny is applied to email attachments and that malware defense begins (but does not end) at the email gateway.

When malware is installed on an already compromised device by way of a direct install, it is highly likely that traditional malware defense can be circumvented. We found that these cases of direct installation were primarily Point of Sale Intrusions where legitimate user credentials were used to access the environment remotely. That can be contrasted with web drive-bye's rely on unpatched browsers and browser plug-ins in order to install the malware on the unsuspecting site visitor.

Malware is a difficult dragon to slay, but as we state in the 2018 DBIR "it does follow some well-trodden paths". It is up to us to make sure the well-trodden is also well defended. Malware detection controls are but a part of a more holistic security strategy that includes strengthening authentication, as well as keeping up with our patch management duties.

Visit www.secretservice.gov to contact your local USSS ECTF.

## SECRET SERVICE AGENT TOPS LIST OF CYBERCRIME INVESTIGATORS

**(New Haven, CT)** The abundance of news reports regarding financial cybercrime may make it seem like a losing battle, but a U.S. Secret Service agent in Connecticut is seen by the financial services industry as someone who knows how to fight back.

Senior Special Agent Brian McCabe has been building partnerships in the law enforcement and banking community for years to thwart complicated financial fraud. Now he is being recognized for his efforts by the Connecticut Chapter of the International Association of Financial Crimes Investigators (IAFCI). McCabe will receive the Chapter's Law Enforcement Officer of the Year Award on June 15, 2018.

"Through Brian's quick actions, he has been able to recover (more than $1 million) of fraudulently wired funds and return the funds to the victims," according to an IAFCI press release.

McCabe is a member of the U.S. Secret Service's Electronic Crimes Task Force and is part of a Connecticut Cyber Working Group that includes federal, state and local law enforcement, and the Connecticut State's Attorney's Office.

Senior Special Agent Brian McCabe exemplifies the investigative talent and work ethic of the Secret Service," said Kenneth Jenkins, Assistant Director, U.S. Secret Service Office of Investigations. "The Secret Service is extremely proud of the work SSA McCabe, and others like him do every day to contribute to the success of our investigative mission."

McCabe is being recognized by IAFCI for his personal involvement in halting five large, wire fraud attempts that began with compromised business email at financial firms. Several cases involved "spoofed" email, where the recipient believed it was a valid request from a trusted partner to transfer funds. McCabe was able to reverse the transfers by getting involved early.

Since financial crimes often involve suspects and entities in many countries, timing is key. McCabe said the U.S. Secret Service leverages domestic and international law enforcement partnerships to stop intricate financial crimes. The effort can often be made easier if funds have not reached countries where partnerships have not been established.

"Banks and firms should establish relationships with local and federal law enforcement prior to becoming a victim, so that they know who to contact regarding a cyber incident or crime,"

McCabe said. “The earlier law enforcement can get involved, the greater chance we have at getting the funds back.”

*For more information on the U.S. Secret Service Electronic Crimes Task Forces, visit https://www.secretservice.gov/investigation/#field*

## Daniel Johnson

This case originated in 2015 when the Billings (MT) Resident Office identified an online identity, who was selling counterfeit US $100.00 Federal Reserve Notes (FRNs) and being paid with Bitcoin. The subsequent investigation revealed the person related to this online identity was Daniel Johnson from Oklahoma. The Oklahoma City Field Office (OKC) conducted an investigation leading to the arrest and subsequent judicial action of Daniel Johnson. Johnson was indicted by a Federal Grand Jury in the Western District of Oklahoma and a Federal Arrest Warrant was issued. Johnson absconded and began living under stolen identities in Oklahoma and Texas. OKC continued the investigation of Johnson and was working with the U.S. Marshal’s Service to locate and arrest Johnson.

In September 2017, the Savannah Resident Office (SAV) initiated an operation that identified an unknown online identity selling counterfeit US $100.00 FRNs. Coordination between the Oklahoma City Field Office, Savannah Resident Office, Criminal Investigative Division, Forensic Services Division and the U.S. Postal Inspectors revealed the person with the same online identity was selling the same counterfeit FRNs for which Daniel Johnson was indicted. Further investigation revealed this online identity was mailing the counterfeit from a post office in Norman, Oklahoma. USSS OKC and US Postal Inspectors in Oklahoma were able to identify Daniel Johnson at a US Post Office in Norman, Oklahoma. Furthermore, the vehicle that Daniel Johnson was driving was identified and data queries revealed the vehicle was registered to a stolen identity. Continuing investigation led to the subsequent search and arrest operation in the OKC District.

In May 2018, agents from the USSS SAV and USPIS SAV flew to Oklahoma City to assist the OKC FO with locating Daniel Johnson. A court order was obtained by OKC FO and served on OnStar to provide tracking information for the 2017 Chevrolet Silverado Johnson was driving. As a result of the OnStar technology, additional addresses were revealed of possible places where Johnson had visited. The information gathered was enough for probable cause for three (3) federal search warrants and one (1) state search warrant. Federal search warrants were signed for the 2017 Chevrolet, an apartment and house that was rented by individuals using several false identities to several properties, one of which was located on 40 acres of land outside of Norman, Oklahoma. The state search warrant was signed for a single-family home in Yukon, Oklahoma rented in one of the fraudulent identities.

Through the coordination of the OKC FO and the US Marshal's Fugitive Task Force, the decision was made to execute the federal arrest of Daniel Johnson on May 17, 2018, followed by the execution of all search warrants. With the help of OnStar, Johnson's vehicle was located and disabled while the USSS and USMS executed a felony vehicle stop in which the subject, Daniel Johnson exited his vehicle and exchanged gunfire with law enforcement. Johnson was shot during the altercation and subsequently died of his injuries on-site. No law enforcement personnel were seriously injured and the crime scene was turned over to the Oklahoma State Police for processing.

As a result of the execution of the federal search warrants the following items were recovered as evidence:

1) $200,000 in counterfeit $100.00 FRNs
2) Various electronic devices
3) Ammonium nitrate
4) Genuine cash
5) Firearms
6) Body armor
7) Detonators
8) Ammunition
9) $45,000 in counterfeit currency
10) Counterfeit paraphernalia

OKC and SAV are in the process of reviewing the evidence. OKC ECTF has conducted examinations of the electronic devices and imaged several hard drives and data storage devices. At this time, the evidence is being examined at USSS Facilities in Oklahoma and Washington, DC. The criminal complaint was unsealed and coordination between the US Attorney's Office in the Southern District of Georgia and the USSS Asset Forfeiture Branch is ongoing to discuss future asset forfeiture in this case.

## Gas Pump Skimmers

The Secret Service, Criminal Investigative Division, Global Investigative Operations Center (GIOC) established strong partnerships with financial institutions to identify and investigate suspected fuel pump skimming locations throughout the United States. From October 2017 to present, the GIOC has identified a total of 800 suspected fuel pump skimming locations and sent that data to Field Offices / Resident Offices via GIOC Intel Alerts. Some of the GIOC Alerts resulted in skimmer recoveries and arrests.

On May 18, 2018, GIOC Alerts were distributed to the field via a SAIC / RAIC email and FOs were tasked with canvasing suspected fuel pump skimmer locations to recover skimmers and dismantle ongoing fraud operations. During this initiative titled, "Fuel Pump Skimmer Disruption Week," the GIOC, working with Financial Institution partners, identified 123 suspected fuel pump skimmer locations.

As of June 11, 2018, participating offices recovered over 73 skimmers from the suspected locations identified by GIOC analysis. Images of the seized skimmers are being sent to the USSS detailees at the National Cyber-Forensics & Training Alliance (NCFTA) for further exploitation. This will enhance the NCFTA skimmer dataset. Furthermore, the recovery of the 73 skimmers increased the overall skimmers seized to 180 since the beginning of FY18. In addition, the data capacity of one (1) skimmer usually depends on the size of the motherboard and type of skimmer. There have been instances where as many as 2000 cards have been on a skimmer but the average is usually between 75 – 200 cards on a skimmer.

GIOC analysts will continue to work with offices interested in developing additional investigative leads to further ongoing respective criminal investigations as well as the ongoing Operation Caribbean Fury.

## DIGITAL SUCCESS STORIES

### National Computer Forensics Institute (NCFI) – The Secret Service's Forensics Force Multiplier


The National Computer Forensics Institute (NCFI) is an excellent example of the Secret Service partnering with the state and local law enforcement community across the United States. The NCFI, located in Hoover, AL, is the nation's only federally funded training center dedicated to instructing state and local law enforcement officers, prosecutors, and judges in digital/cyber-crime investigations. The NCFI was opened in 2008 through collaboration between the U.S. Secret Service, the Department of Homeland Security, and the State of Alabama, with a mandate to provide state and local law enforcement, legal and judicial professionals a free, comprehensive education on current cyber-crime trends, investigative methods, and

prosecutorial challenges. Through nominating our law enforcement partners to attend the NCFI, we are able to help provide state and local law enforcement personnel with the equipment and training they need to efficiently dismantle criminal organizations that are leveraging technology to participate in ALL types of crimes. As a result, NCFI empowers state and local law enforcement to better serve their local communities. Additionally, the NCFI prepares students to become members of the Secret Service's network of 40 ECTFs. Students trained at NCFI are able to immediately join and interoperate with the Secret Service's network of Electronic Crimes Task Forces. So, in the spirit of true partnership, NCFI helps the Secret Service increase our investigative resources while simultaneously enhancing the investigative mission of state and local law enforcement agencies across the country.

From 2008-present, the Secret Service has trained and equipped a total of 7,354 students, including 4,744 state and local law enforcement officers, 2,099 state and local prosecutors, and 511 judicial officials. These students represent all 50 states, three U.S. territories, over 2,000 agencies nationwide, and strengthen the Secret Service's network of 40 Electronic Crimes Task Forces. In Fiscal Year 2017, NCFI graduates conducted approximately 40,000 forensics exams. More specifically, through our Forensic Partner Reporting (FRP) system, over 11,000 exams were conducted for cases involving missing and exploited children and child pornography. Approximately 4,000 exams were conducted involving murder investigations; over 3,900 exams involving drug related investigations; and over 2,600 exams involving rape investigations were conducted.

Based on these successes, the NCFI's strategic goal is to reach maximum training capacity so that we can provide more training opportunities for our partners. The Secret Service assesses that it could train over 3,100 law enforcement personnel per year at the existing NCFI facility is fully funded. Therefore, the Secret Service is prepared to execute a five year growth plan to reach this level, if provided sufficient funding. Despite strong support from DHS and Congress for this program, the primary constraint to NCFI growth has been an Office of Management and Budget (OMB) concern of a lack of an explicit authorization. On November 2, 2017, President Trump signed into law H.R. 1616, the "Strengthening State and Local Cyber Crime Fighting Act of 2017," which received overwhelming support in the House and Senate. This bill formally authorizes the Secret Service to operate the NCFI for fiscal years 2017 through 2022. In short, this legislative action codifies into law the existing relationship between the Secret Service and NCFI and demonstrates continued confidence in the Secret Service operating this critical program. This authorization bill establishes the foundation for NCFI growth over the next five years to operating at full capacity of 3,100 law enforcement personnel per year.
The following story is a testament that the partnership between Federal, State and local law enforcement agencies and why the NCFI is an important resource used to combat various types of crimes:

On April 13, 2018, the parents of twenty-one year old female reported to the Waukesha Police Department that their daughter had been missing. The parents told police that their daughter failed to pick up her brother from school and failed to show up for her work shift which made them concerned.

The female's boyfriend, advised the parents that he had not seen her and didn't know where she was. When the parents allegedly told him that they were going to the police, he seemed uneasy and said he wouldn't go along.

During the course of the investigation, the family turned over an Apple watch that had some messages on it, indicating she was supposed to meet her boyfriend earlier that day. A MacBook Pro was also turned over which was logged into her iCloud account – capturing all of the iMessages that were synced between devices.

Detective Michael Carpenter, Waukesha Police Department, recently attended MAC Forensic Training at the Nation Computer Forensic Institute (NCFI) which provided him Apple specific tools and training. Det. Carpenter states, "Prior to this we did not have any tools to conduct Apple specific exams. I was able to image and process the Mac and locate thousands of messages between the victim and her boyfriend over a seven month period. These messages detailed past abuse and the problems this couple was having. The information located on these exams showed the boyfriend was not being truthful about that last time he saw the victim and allowed us to acquire a probation warrant and take the boyfriend into custody. His iPhone was then examined, where deleted web searches were found indicating the suspect was researching methods consistent with attempting to dispose of a body."

The suspect and the investigation were turned over to the Milwaukee Police Department. Utilizing the information obtained from the timely forensic examination on the computer, a search warrant was obtained for the suspect's residence. The crime scene was located which allowed investigators to further interview the suspect and obtain a confession. The suspect described the circumstances surrounding the murder and the location of the victim's remains.

Det. Carpenter advises that "From the time she was first reported missing to the time her body was recovered was approximately 30 hours. The tools and training from NCFI allowed us to immediately begin this investigation in a timely matter. Had I not obtained this training it would have taken much longer to properly examine these devices and establish probable cause? The suspect was charged with First Degree Intentional Homicide, First Degree Intentional Homicide of an Unborn Child, and Felon in Possession of a Firearm.

Thank you for all you do and the excellent training and equipment you provide. It is greatly appreciated and has a direct impact on our investigations."

In an effort to show our appreciation and recognize our state and local partners that have been NCFI trained and are actively participating in our Forensic Partner Reporting (FPRs) system, the Secret Service recently recognized several of our partners for their outstanding efforts during fiscal year 2017.


***Photo Courtesy of the U.S. Secret Service, St. Louis Field Office***

2017 NCFI Top Examiner Award presented to Forensic Examiner Detective Mike Slaughter, Special Investigations Unit, St. Louis County, MO Police Department. Mr. Slaughter was presented with the award by A/SAIC Trevor Fenwick, U.S. Secret Service, St. Louis Field Office and Detective Sgt. Adam Kavanaugh, St. Louis County, MO Police Department.

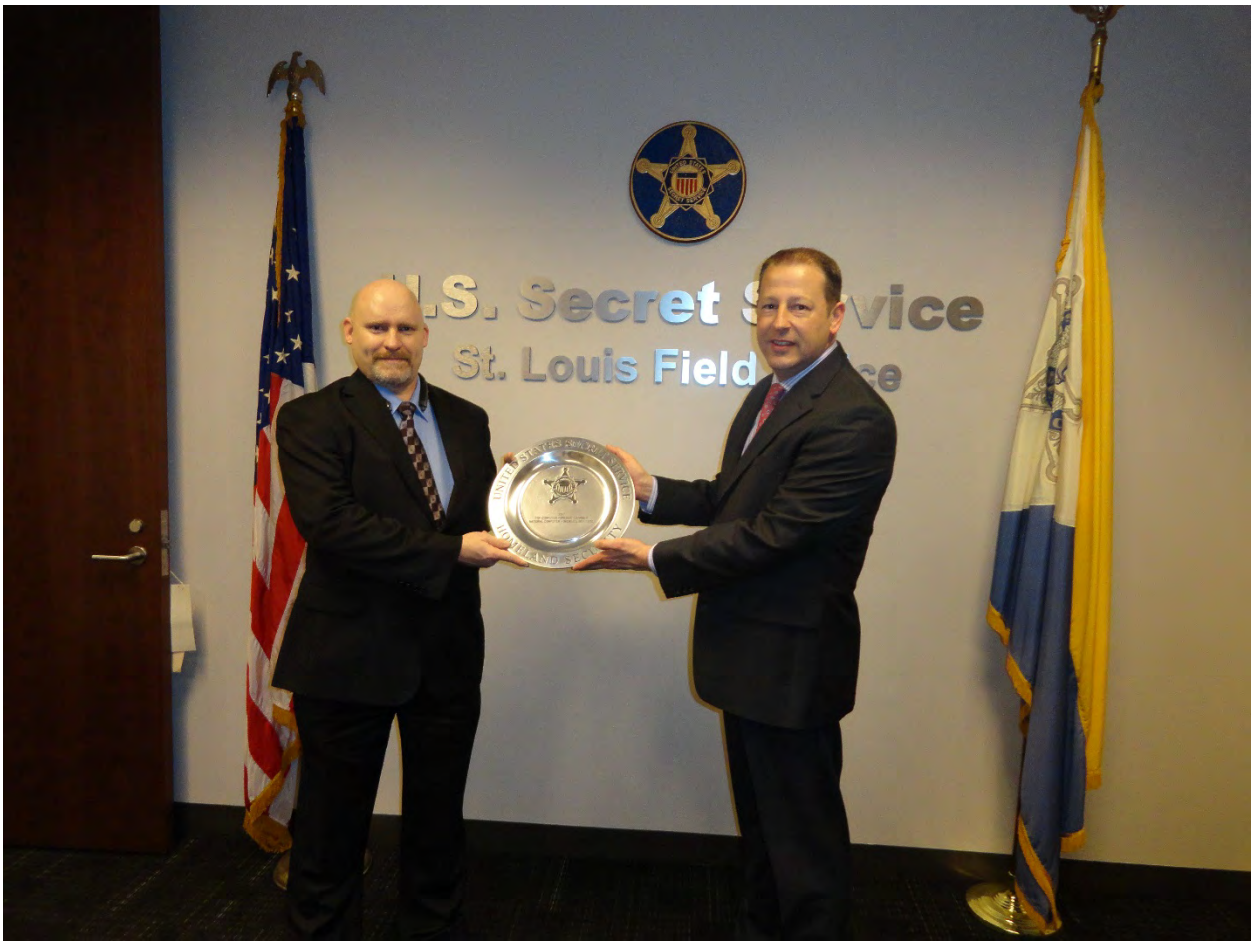



***Photo Courtesy of the U.S. Secret Service, St. Louis Field Office***

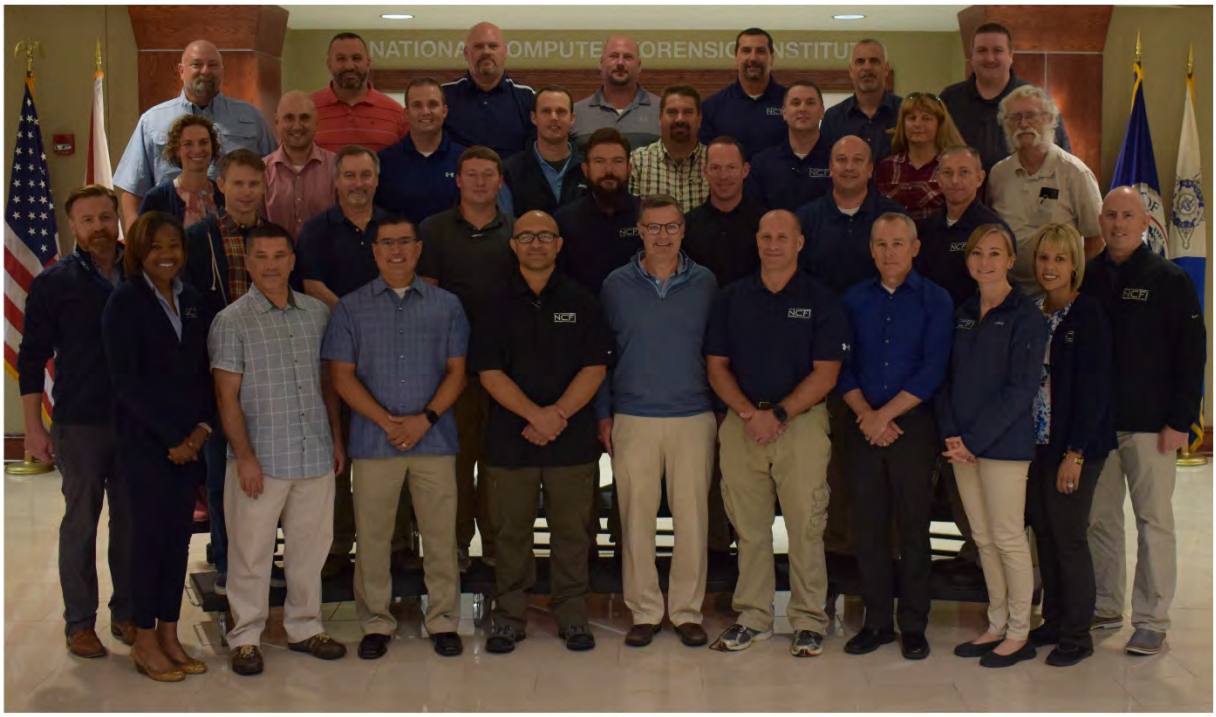
2017 NCFI Top Examiner Award presented to Forensic Examiner Detective Bobby Baine, (Retired – Jan 2018), St. Louis Metropolitan, MO Police Department. Mr. Baine was presented with the award by A/SAIC Trevor Fenwick, U.S. Secret Service, St. Louis Field Office.


***Photo Courtesy of the U.S. Secret Service, Washington Field Office***

2017 NCFI Top Examiner Award presented to Forensic Examiner Detective William Heverly, Montgomery County, MD Police Department. Mr. Heverly was presented with the award by ASAIC Nathaniel Davis, U.S. Secret Service, Washington Field Office.

***Photo Courtesy of the U.S. Secret Service, Denver Field Office***

2017 NCFI Top Examiner Award presented to Forensic Examiner Investigator Mike Garnsey, Arapahoe County Sheriff's Office, CO Police Department. Mr. Garnsey was presented with the award by SAIC John Gullickson U.S. Secret Service, Denver Field Office.



**NATIONAL COMPUTER FORENSICS INSTITUTE**

2017 Forensic Partner Award Winners
Memory Forensics Training
May 15-18, 2018
*Hoover, AL*

For additional information on the National Computer Forensics Institute, to include upcoming scheduled class offerings and eligibility, please visit **https://www.ncfi.usss.gov/ncfi/.**

## CYBER OUTREACH

### The National Cyber-Forensics and Training Alliance

What can the NCFTA do for you?

The National Cyber-Forensics & Training Alliance (NCFTA) is a non-profit corporation founded in 2002, focused on identifying, mitigating, and neutralizing cyber-crime threats globally. The NCFTA was created by industry and law enforcement for the sole purpose of establishing a neutral, trusted environment that enables two-way information sharing with the ultimate goal to identify, mitigate, disrupt, and neutralize cyber threats. By working across multiple industry

sectors and agencies, NCFTA is able to identify, mitigate, and ultimately defeat significant domestic and global cyber threats. In 2017, satellite offices were opened in New York, NY and Los Angeles, CA.

The USSS currently has four personnel assigned to the NCFTA; IT Specialist Christopher Vaccarello, IA Hannah Feldman, SA Vacant (Pittsburgh, PA), and ATSAIC Kevin McCleary (New York, NY). The USSS has been located at NCFTA offices since November, 2014.

Law Enforcement Partners: FBI, HSI, CBP, U.S. Postal Inspection Service, IRS CID, DEA, Europol, LA County Prosecutor's Office, District Attorney of New York (DANY).

**Resources for USSS Investigations – What can we do for you!**

There are three types of searches that USSS personnel can run for you at NCFTA. They are as follows:

1. ***Passive Search*** – search of USSS Case Search, Liberty Reserve, NIAC data, as well as NCFTA datasets (No external notification of case data)

2. ***Law Enforcement Search*** – pertinent case data shared with other FED LE partners (FBI, CBP, HSI, USPIS) (Not shared with corporate sector partners)

3. ***NCFTA Partner Listserv query*** – pertinent case data shared across Financial Institutions/Retailers/Other FED LE agencies to query their data (External notification of case data)

**Overview of Tools/Programs:**

***USSS Case Search Tool*** – allows for quick and bulk data searches against historic investigative case Memorandums of Record from the time period 10/10/2000 to present.

***Network Intrusion Action Center (NIAC) Search Tool*** – allows for quick and bulk data searches against all current and historic FIRS entries made into the NIAC from 8/4/2016 to present.

***Liberty Reserve (LR) Database Search Tool*** – allows for quick and bulk data searches against the LR database. It is noted that results from the LR database must be treated as intelligence only and cannot be shared outside the USSS without the concurrence of NYFO and CID.

***Common Point of Purchase (CPP) Reports*** – An analysis report listing the CPP's identified is currently distributed to the ECTFSUPS and NITRO email routers on a weekly basis. These reports are an aggregation of data by 11 reporting financial institutions to identify CPP's where initial fraud/compromise may have occurred. These reports can be utilized by the fields for both incident response and case development.

***Internet Fraud Alert (IFA)*** – IFA is a centralized clearinghouse and alerting mechanism for reporting compromised credentials (credit card #'s, email addresses and associated passwords) discovered online or during the course of an investigation. Compromised credentials obtained during an investigation can be provided to IFA, via the USSS NCFTA personnel. Additionally, a list of contacts for the affected financial institutions will be provided to the case agent for further investigation.

***ATM Skimming Working Group*** – NCFTA maintains a database of ATM and fuel pump skimming incidents which have been reported by either law enforcement or financial institution partners. CCTV photographs of both known and unknown subjects are manually compared in order to make identifications and link organized groups.


## *When Piggy Back Warrants for Electronically Stored Information Are Necessary*

**United States v. Hulscher**

A Federal District Court has recently ruled that a law enforcement agency cannot conduct a subsequent search of seized digital evidence that is unresponsive to the original search warrant. In *United States v. Hulscher*, 2017 U.S. Dist. LEXIS 22874 (D.S.D. 2017), a local law enforcement agency seized and copied the contents of a defendant's cell phone pursuant to a search warrant that was issued for forgery, counterfeiting, and identity theft charges. The local law enforcement agency segregated the contents of the cell phone into data that was responsive to the search warrant and data that was not responsive to the search warrant. Subsequently, the Bureau of Alcohol, Tobacco and Firearms (ATF) requested and received from the local law enforcement agency a complete copy of the contents of the defendant's cell phone, including data that was not responsive to the original search warrant, to assist with its investigation into federal firearms charges. ATF did not receive a second search warrant before searching the contents of the cell phone.

The district court held that:

1) The subsequent viewing of a copy of electronic data from a cell phone constitutes a search when the data was collected under a valid search warrant but was unresponsive to that warrant, concluding "[t]he government's position, which would allow for mass retention of unresponsive cell phone data, is simply inconsistent with the protections of the Fourth Amendment;" and

2) The plain view exception to the Fourth Amendment did not apply to the search, because the ATF did not have sufficient justification at the outset to search the non-responsive cell phone data. *See also United States v. Stierhoff*, 477 F. Supp. 2d 423 (D.R.I. 2007) (the

plain view doctrine does not allow an investigator to search through a computer hard driver folder other than the one he had been given consent to search).

**United States v. Huntoon**

The facts at issue in *Hulscher* can be usefully contrasted with the facts at issue in *United States v. Huntoon*, 2018 U.S. Dist. LEXIS 61992 (D. Ariz. 2018). In this case, HSI acquired a defendant's laptop from a local law enforcement agency and conducted a subsequent search of the laptop. HSI's search for evidence was related to child pornography. The court held that this search did not interfere with the defendant's Fourth Amendment rights, because the original search warrant for the laptop authorized the local law enforcement agency to search for evidence related to child pornography. The decision concluded that "[t]here is ample case law to support the Government's position that a second warrant to search a properly seized computer is not necessary as long as the subsequent search does not exceed the probable cause articulated in the original warrant."

For questions or additional information, please contact Attorney Advisor Steven Giballa at steven.giballa@usss.dhs.gov or 202-406-5659.

**Department of Homeland Security Cybersecurity Strategy**

On May 15, 2018, Secretary Nielson announced the release of the Department of Homeland Security *Cybersecurity Strategy*, which outlines the Department's approach to identifying and managing national cybersecurity risks. The strategy sets forth five pillars to achieving seven desired goals; most relevant to the U.S. Secret Service's integrated mission is *Pillar Three: Threat Reduction / Goal Four: Prevent and Disrupt Criminal Use of Cyberspace*, which prioritizes efforts "to pursue, counter, reduce, and disrupt illicit cyber activity" and call for "closer collaboration with other federal, state, local, and international law enforcement partners," the hallmarks of the Secret Service's Electronic Crimes Task Force model. The document strongly reaffirms the importance of the Secret Service's efforts to improve cybersecurity by: 1) identifying risk, 2) reducing cyber vulnerabilities, 3) reducing cyber threat by preventing and disrupting criminal use of cyberspace, 4) assisting in responding effectively to cyber incidents, and 5) working with partners to improve cybersecurity risk management.
DHS will issue a more detailed "Implementation Plan" for the strategy in the coming months that will inform the Department's future budget, planning, training, and programming activities. The U.S. Secret Service's Office of Investigations is working in close coordination with other DHS components on this effort.

For questions or additional information, please contact Management and Program Analyst Jonah Hill at jonah.hill@usss.dhs.gov or 202-406-5048.

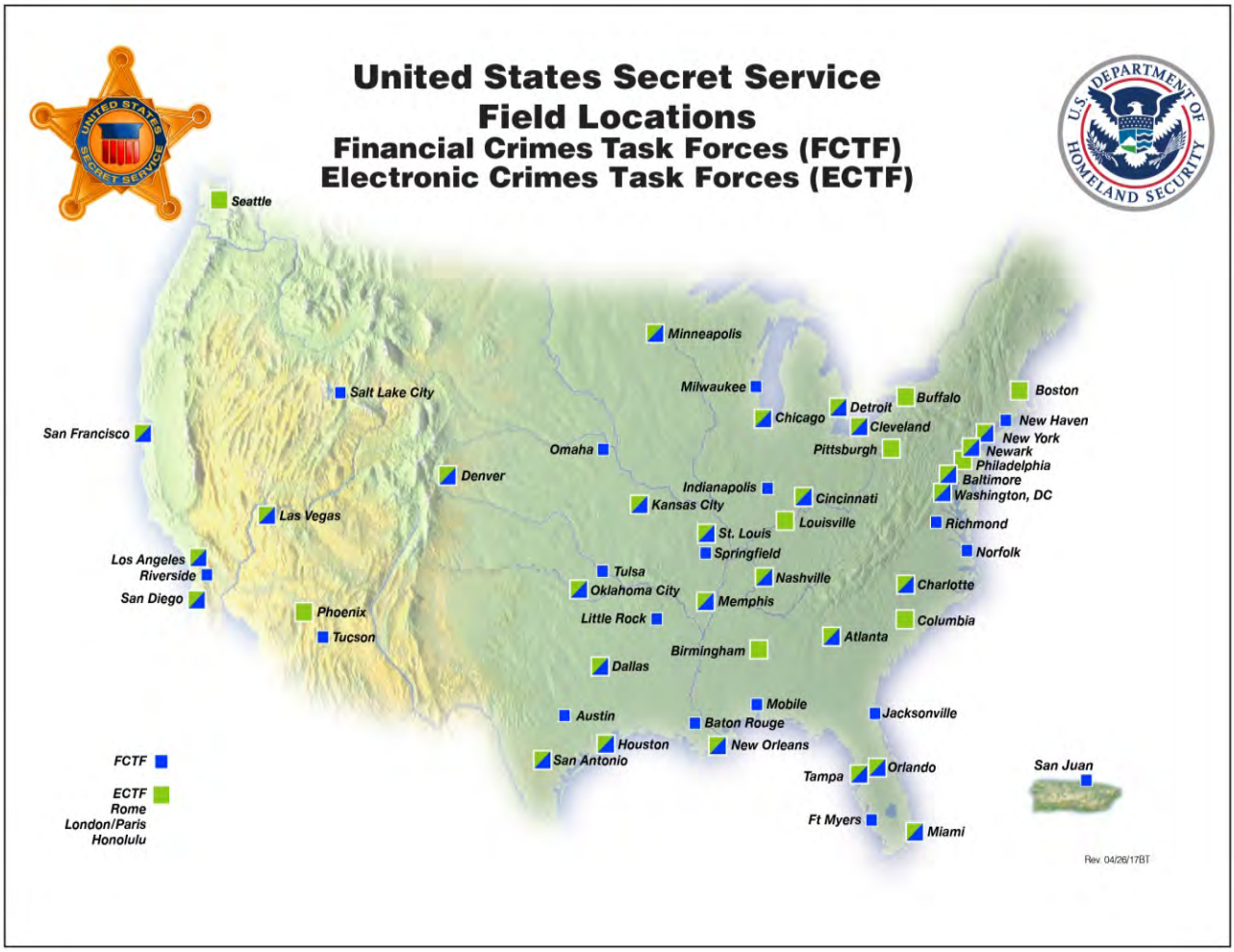

Atlanta, GA
404-331-6111
Baltimore, MD
443-263-1100
Birmingham, AL
205-731-1144
Boston, MA
617-565-5640
Buffalo, NY
716-551-4401
Charlotte, NC
704-442-8370
Chicago, IL
312-353-5431
Cincinnati, OH
513-684-3585
Cleveland, OH
216-750-2058
Columbia, SC
803-772-4015

Dallas, TX
972-868-3200
Denver, CO
303-850-2700
Detroit, MI
313-226-6400
Honolulu, HI
808-541-1912
Houston, TX
713-868-2299
Kansas City, MO
816-460-0600
Las Vegas, NV
702-868-3000
Los Angeles, CA
213-894-4830
Louisville, KY
502-582-5171
Memphis, TN
901-544-0333

Miami, FL
305-863-5000
Minneapolis, MN
612-348-1800
Nashville, TN
615-736-5841
Newark, NJ
973-971-3100
New Orleans, LA
504-841-3260
New York, NY
718-840-1000
Oklahoma City, OK
405-272-0630
Orlando, FL
407-648-6333
Philadelphia, PA
215-861-3300
Phoenix, AZ
602-640-5580

Pittsburgh, PA
412-281-7825
San Antonio, TX
210-308-6220
San Diego, CA
619-557-5640
San Francisco, CA
415-576-1210
Seattle, WA
206-553-1922
St. Louis, MO
314-539-2238
Tampa, FL
813-228-2636
Washington, DC
202-406-8000

London, England
Rome, Italy


United States Secret Service
Field Locations
Financial Crimes Task Forces (FCTF)
Electronic Crimes Task Forces (ECTF)
Seattle
Minneapolis
Salt Lake City
Milwaukee
Buffalo
Boston
Detroit
Chicago
New Haven
Cleveland
New York
San Francisco
Omaha
Pittsburgh
Newark
Philadelphia
Denver
Indianapolis
Baltimore
Cincinnati
Washington, DC
Kansas City
Las Vegas
Louisville
Richmond
St. Louis
Springfield
Norfolk
Los Angeles
Riverside
Tulsa
Nashville
Charlotte
San Diego
Oklahoma City
Memphis
Phoenix
Little Rock
Columbia
Tucson
Atlanta
Birmingham
Dallas
Mobile
Austin
Jacksonville
Baton Rouge
Houston
New Orleans
San Antonio
San Juan
Orlando
Tampa
FCTF
ECTF
Rome
London/Paris
Honolulu
Ft Myers
Miami
Rev. 04/26/17BT